TLP:WHITE

February 2024

Critical Infrastructure Interdependencies

“Pull a thread here and you’ll find it’s attached to the rest of the world.”

—Nadeem Aslam, The Wasted Vigil

Health-ISAC™

SHARING SINCE 2010

Collaborating for Resilience in Healthcare

TLP:WHITE This report may be shared without restriction. For Health-ISAC members—be sure to download the full version of the report from the Health-ISAC Threat Intelligence Portal (HTIP). Contact Membership Services for assistance.

health-isac.org

Contents

Key Judgements

- Interconnectedness has resulted in interdependence. Therefore, critical infrastructure should be treated as a singular entity from a security perspective.
- Threat actors capitalize on single-point-of-failures in successful attacks.
- Critical Infrastructure faces a unique security dilemma: expanding outreach while decreasing volatility.
- Redundancy, in both architecture and knowledge, is the key to critical infrastructure security.
- Breaking down the silos of information sharing across critical infrastructure security communities is vital to collective success.
- Disaster Recovery (DR) and Business Continuity (BC) planning should incorporate inbound and outbound dependencies.

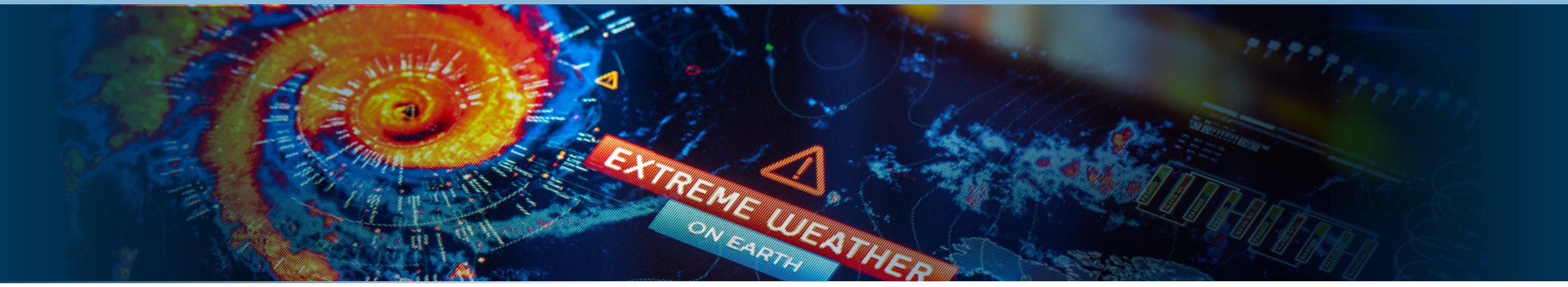
Introduction

The definition of critical infrastructure may vary from country to country, but it's safe to say that critical infrastructure is what governments consider essential for the functioning of society and the economy. INTERPOL (the world's largest international police organization) asserts that regardless of definition, these sectors must be effectively protected from attacks[1]. Both the European Union and the United States have included healthcare as part of their respective critical infrastructure (CI)[2]. However, the healthcare sector needs other critical infrastructure sectors to operate and sustain operative conditions. Healthcare, like all other critical infrastructure, is dependent upon other sectors. For instance, if there were an interruption in electricity, manufacturing assembly lines would not be able to function, thus causing shortages in medication which would impact the ability of healthcare providers to serve their patients; but without a healthy workforce, the energy sector would have no way of functioning. This phenomenon is known as interdependence. The term single point of failure is a term often used to visualize cascading consequences. In this context, it also applies to critical infrastructure. The analogy is as follows: A chain is made up of many different links. Should any one of those links break, the entire chain will fall apart, regardless of how large it is. Due to the interdependencies of critical infrastructure, if one sector experiences an outage, the entire ecosystem suffers a decrease in productivity or an outright outage.

This paper is designed to provide decision-makers with information to make threat-informed decisions regarding resource allocation toward security in critical infrastructure organizations. In a world of ever-evolving threats, both cyber and physical, it is crucial for organizations in critical sectors to be cognizant of the scale of sector interdependence and incorporate it into disaster recovery (DR) and business continuity (BC) planning. This white paper seeks to provide the reader with the knowledge necessary to begin the accession of dependency-based risk analysis into the larger DR/BC schema.

[1] INTERPOL. (2017, September 20). UNSCR 2341 (2017) and the Role of Civil Aviation in Protecting Critical Infrastructure from Terrorist Attacks. https://www.icao.int/. Retrieved August 22, 2023, from https://www.icao.int/Meetings/AVSEC2019/Documents/CI%20Workshop_Interpol.pdf

[2] The SPEAR Project. (2021, March 16). A Review of Critical Infrastructure Domains in Europe. Retrieved August 18, 2023, from https://www.spear2020.eu/News/Details?id=120



Infrastructure Volatility

Energy is one of the most crucial sectors of critical infrastructure as nearly everything relies on power in Western society; however, it has the most reported failures[3]. In the event of a storm or other abnormal weather conditions, the power is liable to go out. When power is out at peoples' homes, the cascading impacts can be felt directly by the residents. Often, flashlights must be used for light, and the internet will be unavailable for a time. Should this issue persist, perishable foods may go bad and may need to be removed from the refrigerator and freezer.

For the healthcare sector, a power outage means much more than flashlights and possible spoiled food, but rather the consequences range from destruction of research and possible contamination in life sciences to potential loss of life in healthcare delivery organizations.

Targeted attacks against supply chains can have widespread consequences that affect all levels of industry. A cyber-attack on a major Japanese shipping port exemplified this concept in mid 2023.

In July 2023, the largest port in Japan was hit with a ransomware attack, resulting in a complete shutdown of operations. The port could not accept shipments for the next two days following the incident[4]. This likely delayed shipments of medical devices to hospitals and caused shortages of personal protective equipment (PPE) for healthcare providers. Incidents such as this show how quickly the consequences of attacks on critical infrastructure can cascade when the web of interdependency is rattled.

On January 25, 2021, hackers were able to infiltrate the internal network at WestRock manufacturing, causing a major slowdown in operations. This was due to the operational technology (OT) systems controlling the robotics in the facility being affected by the ransomware.[5] WestRock had many pharmaceutical clients that relied on its packaging services to ship products worldwide. The incident was resolved on February 4, 2021, however, the company suffered major production setbacks during the period between the attack and the resolution. On February 5, WestRock stated its mill system production during the incident was 85,000 tons lower than planned. This likely led to drug and PPE shortages for healthcare delivery organizations and retailers, thus highlighting the ripple effect of attacks against supply chain entities.

At the beginning of the Russia-Ukraine war in early 2021, a Russian nation-state threat actor attacked Viasat modems to obstruct broadband satellite internet access. While the attack was aimed at disrupting Ukrainian military and government telecommunications, many rural areas that relied on satellite internet were affected, too. Additionally, a German energy company lost access to over 5,800 wind turbines deployed in remote areas and an internet service provider in France with 9,000 customers shut down. The lack of connectivity and energy resources likely created a situation where healthcare entities received less energy than they typically do, resulting in the temporary loss of some services to compensate for the sudden decrease in resources. Events such as these highlight the likelihood of collateral damage from critical infrastructure outages to span beyond national borders[6].

[3] Macaulay, T. (2019, May 9). The danger of critical infrastructure interdependency. Centre for International Governance Innovation. https://www.cigionline.org/articles/danger-critical-infrastructure-interdependency/

[4] Japan's largest port hit with ransomware attack. (n.d.). CNN. https://www.cnnphilippines.com/business/2023/7/7/port-of-nagoya-ransomware-attack.html

[5] Dinu, C. (2021, May 6). Westrock Ransomware Attack: A quick guide. Heimdal Security Blog. https://heimdalsecurity.com/blog/westrock-ransomware-attack/

[6] Viasat Case study: Viasat attack: CyberPeace Institute. Viasat Attack | CyberPeace Institute. (n.d.). https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat#impact

Critical Infrastructure Interdependencies Matrix

This Critical Infrastructure Interdependencies Matrix[3] was developed by the Center for International Governance Innovation (CIGI), a Canadian think tank that highlights security issues to improve governance. This matrix uses the ten critical infrastructure sectors of Canada, where public safety is denoted as safety. This critical infrastructure risk matrix exemplifies interdependence among the sectors of critical infrastructure. The columns in this graph represent how much a given sector of critical infrastructure relies on information given by another sector. For example, healthcare rated its dependency on information on food at 3.76/10. The rows represent how dependent other sectors of critical infrastructure sectors are on information provided by a given CI sector. For IT and Communications' dependency on information coming from the healthcare sector was scored as 2.43/10. The cells highlighted in blue represent how dependent a given sector of critical infrastructure is on itself. For example, Healthcare rated its dependency on itself as 8.25/10.

Inbound Dependencies

Outbound Dependencies

Critical Infrastructure Sector	Energy	Communications & IT	Finance	Healthcare	Food	Water	Transportation	Safety	Government	Manufacturing
Energy	9.37	3.63	2.48	3.88	2.06	3.08	4.25	3.23	3.36	3.24
Communications & IT	6.96	8.82	4.48	5.11	2.32	3.42	4.41	4.62	3.96	7.08
Finance	7.13	7.19	8.95	4.23	8.23	5.01	6.78	4.02	5.18	7.96
Healthcare	4.12	2.43	2.99	8.25	1.80	4.43	3.33	5.78	5.06	2.57
Food	1.47	1.66	1.94	3.76	6.45	1.83	2.48	1.05	2.71	1.99
Water	4.90	1.84	1.96	3.60	1.30	5.78	3.18	1.2	2.87	2.16
Transportation	6.82	3.95	4.23	4.95	5.06	2.96	7.49	3.78	4.66	5.84
Safety	7.85	3.96	3.6	5.71	1.02	4.54	5.35	8.23	5.73	4.96
Government	5.85	5.05	7.00	6.12	4.76	5.05	7.61	6.43	8.78	5.96
Manufacturing	5.87	3.75	4.66	5.01	4.50	3.43	4.53	1.17	3.63	7.15

Center for International Governance Innovation

The consequences of a power outage are well-documented and a routine occurrence for many. While common, they are difficult to predict. However, due to the size and scale of energy infrastructure, unorthodox causes such as sabotage, reckless driving, excavation efforts, and even squirrels often result in severe power outages.

Therein lies the inherent issue with utility-providing sectors of critical infrastructure. The customer bases of these sectors are massive as they provide necessities for modern societal living. With an infrastructure so vast, volatility is inevitable. The interconnectedness of it is a necessary risk because it is impossible for critical infrastructure to function at its current efficiency without interdependence. However, interdependence also increases the CI attack surface. Interconnected webs of critical infrastructure are so dense it is usually described as a singular entity because an attack on one critical sector spells trouble for the rest. While the dependence one sector has on another varies, the dependence exists. Therefore, the consequences that will arise from a failure in one sector will cascade to the others.

To exemplify critical infrastructure risk being mitigated as a single entity, the US Transport Security Administration (TSA) secures American airports as a single whole rather than having each airline create its own security apparatus. Just as airports represent separate institutions that work together for the common goal of safe transportation, collaborative initiatives such as the National Council of ISACs (NCI), and its sector-specific information sharing and analysis centers (ISACs) members, help various institutions within critical infrastructure accomplish a common goal of security. While the sectors of critical infrastructure prioritize different security incidents, participation in information-sharing organizations help CI entities obtain a broad view of the entire critical infrastructure threat landscape regardless of what sector they operate in. To learn more about the NCI and its function, click here.

This connectedness allows for rapid remediation and quick restoration when disruptions occur in critical infrastructure. The volatility that comes with the massive attack surface of critical infrastructure highlights the need for rapid remediation and secure posturing. Information-sharing organizations can play a crucial part in providing a medium to obtain sector-specific security insights and facilitating coordination with public sector authorities to expedite remediation when security measures fail.

ATLAS is a system developed by Health-ISAC and Cyware to increase collaboration and partnerships between information-sharing communities. ATLAS allows analysts from different sectors of critical infrastructure, as well as international computer emergency response teams (CERTs), to come together and discuss threats facing their respective sectors and coauthor joint bulletins and white papers[7]. ATLAS facilitates ISAC to ISAC analyst information sharing and is open for just about any ISAC, ISAO, CERT or information-sharing body to join. Analyst exchanges such as ATLAS especially benefit smaller critical infrastructure owners that may not enjoy the same security budgets as the larger players in their sector by allowing analysts to acquire insights obtained using sophisticated tools that otherwise may have not been accessible. Email contact@h-isac.org if you are interested in learning more about ATLAS.

[7] Health-ISAC. (2023, July 18). Europe - Health-ISAC - Health Information Sharing and Analysis Center. Health-ISAC - Health Information Sharing and Analysis Center. https://h-isac.org/europe/

Risk Management

The previous matrix outlines a basic risk hierarchy for each sector of critical infrastructure and how it can be used as a starting point to create Disaster Recovery (DR) and Business Continuity (BC) plans. However, it may also be pertinent for the reader to assess inbound data dependencies for their organizations to drive optimized tabletop exercises targeting the top inbound dependencies. Short-term risk mitigation strategies may focus on adapting to certain scenarios or situations, while longer-term risk management strategies study recovery efforts when organizations are cut off from their largest inbound dependency. Black swan incidents are events that are extremely rare but catastrophic such as the Twin Towers collapsing due to terrorists flying planes into them. Following that incident, there was a nationwide grounding of air travel in the United States and critical infrastructure security became a mainstream topic. These scenarios are extremely difficult to plan for as they reside on the fringes of the spectrum of risk management yet remain pivotal to a mature security management portfolio. As black swan events, the incidents themselves are extremely difficult to plan for and remediate. However, the cascading impacts do not share the same atmosphere of mysticism. Major disruptions in transportation, communications, and utilities are all things that can be planned for. These disruptions are often where the true scope of damage caused by black swan events is realized. For example, when COVID-19 hit, supply chains quickly became overwhelmed and were unable to keep up with the demand for masks, and Personal Protective Equipment (PPE), thus causing massive shortages at healthcare facilities across the globe. Simultaneously, cybercrime against healthcare was on the rise, placing patients and clinical staff in an even more precarious position.

Those in risk management positions should not rely on single-threaded static analysis because the idea of such simplicity in society today is obsolete as a result of modern interconnectedness. A more comprehensive approach is required to appropriately address the current risk landscape. Whether the consequences directly hit an organization or indirectly through interdependence, cascading impacts from incidents in CI are inevitable; therefore, it is imperative risk professionals actively consider how an incident could ripple through other sectors as well.

Using the CIGI matrix above, a healthcare executive drafting a proposal for a Tabletop Exercise (TTX) may want to simulate the isolation from the top three inbound information dependencies: Healthcare, Government, and Public Safety, respectively. The higher the inbound data dependence, the more impact an outage would have. Therefore, this TTX would include scenarios where communications with other hospitals, government entities, and emergency services are cut off. The outcome of this discussion can be used to structure DR and BC plans. As a starting point for an internal incident response plan, organizations can use the Coordinated Healthcare Incident Response Plan template written by the Healthcare and Public Health Sector Coordinating Council (HSCC). Additionally, Health-ISAC offers its Tabletop Exercise as a Service (TTXaaS) as a way to supplement member security teams. This program puts on healthcare-specific, intel-driven tabletop exercises for members. Members can pick one of three options: Pre-Defined exercises based off threats observed against the Healthcare Sector, a uniquely tailored exercise with no Quick Look Report, and a uniquely tailored exercise with a Quick Look Report. A Quick Look Report is a brief synopsis of the Tabletop Exercise (TTX), its structure and outcomes. It serves as a condensed version of the TTX experience and relays critical findings in a condensed manner. These reports are ideal to spread awareness of the lessons learned during the exercise to security professionals who were not present during the TTX, or a good reference for those who were present.

Inflated Consequences Due to Critical Infrastructure Interdependence

Interconnectedness, while necessary for an efficient society, also leads to a significant increase in unpredictability from increased volatility. This has led to some unorthodox causes of massive outages, the consequences of which were amplified because of the interdependence of critical infrastructure. Some examples include a massive power outage affecting thousands caused by a squirrel and the grounding of a fleet of aircraft due to four snapped cables miles away from the airport where they were housed[8].

On February 16, 2023, a major energy provider in the state of Florida released a statement regarding a power outage that affected thousands of customers in Lake Mary. This outage, unlike others caused by storms, or large-scale weather events, was caused by a squirrel coming into contact with a power line near the Lake Mary substation. A seemingly insignificant event triggered an outage in the area because of the interconnectedness of modern-day critical infrastructure architecture. This is one of many incidents where the increased volatility of an interconnected ecosystem is highlighted.

Another incident that exemplifies this volatility is the grounding of the German airline Lufthansa at the airport in Frankfurt, Germany, on February 15, 2023. The grounding occurred following the severing of four subterranean cables. The damaged cables were broadband cables that crippled the IT infrastructure for Lufthansa when cut. These cables were at the Deutsche Bahn Railtrack in the Frankfurt region during routine concrete drilling. Once again, the interconnectedness of the critical infrastructure inflated the consequences of a small-scale issue to catastrophic proportions.

These incidents can often snowball into much larger incidents through unforeseen complications. On January 11, 2018, a county-run hospital in Hancock County, Indiana, was hit by a ransomware attack at 9:30 pm during a snowstorm. Systems were acting slower than usual when a message popped up on one of the screens at the hospital stating that devices and the files within were all encrypted and inaccessible to staff. Not only were patients unable to receive care, but ambulances had to be rerouted to surrounding hospitals, potentially delaying care.

Another example of this phenomenon is the intravenous (IV) bag shortage that stemmed from Hurricane Maria making landfall in Puerto Rico on September 20, 2017. When the hurricane hit, it flooded IV bag manufacturing facilities with wastewater, which halted the production of IV bags, leading to a prolonged shortage of bags in the domestic United States[9]. Puerto Rico represented a concentration of risk that was known by few people because the manufacturing presence on the island was crucial to multiple different sectors of critical infrastructure. Because these sectors tend to be siloed off from each other, the true concentration of risk was not known until after Hurricane Maria. The substantial pharmaceutical and medical supply chain on the island were depended on by a multitude of healthcare logistics entities in the domestic United States.

[8] Timmins, B. B. (2023, February 15). Lufthansa tech failure leaves planes grounded. BBC News. https://www.bbc.com/news/business-64652835

[9] Scutti, S. (2018, January 17). IV bags in short supply across US after Hurricane Maria. CNN. https://www.cnn.com/2018/01/16/health/iv-bag-shortage/index.html

Hurricane Maria in Puerto Rico highlights the importance of understanding concentration of risk and the cascading consequences that can arise from the jeopardization of downstream supply chain entities. These concentrations are often difficult to identify, but some indicators are visible.

Manufacturing is an industry that services clients in nearly every industry. Regions with a heavy manufacturing presence are likely inconspicuous concentrations of risk. Therefore, organizations should conduct thorough upstream supply chain risk analysis to identify key points of risk with little redundancy. Once these locations are identified, weather advisories will likely become significantly more important. This holds especially true when key manufacturing facilities are located in less developed countries with less environmentally resistant structures.

When It All Goes Wrong: Five Days at Memorial Medical Hospital

Memorial Medical Hospital, a hospital in New Orleans, was the victim of a total power outage during the 2005 Hurricane Katrina. A massive flood occurred that destroyed backup generators and caused a total outage. This increased the internal temperature of the hospital beyond 100° Fahrenheit (38° Celsius). The hospital remained in this isolated state for five days before evacuation from August 28 to September 1, 2005. Memorial Medical Hospital was left without power, lights, sewer systems, and air conditioning. Medical equipment was rendered inoperable.

Evacuation was impossible as the bottom floor of the building was flooded, preventing egress. When faced with this daunting situation, physicians and staff adopted an unorthodox method of medical triage in which the critically ill patients with do-not-resuscitate (DNR) orders were deprioritized. Trapped within the sweltering building, a makeshift morgue was established to house deceased patients. The number of bodies in the morgue reached 45 by the fifth day after euthanasia was performed on critically ill patients, which doctors believed would not survive the ordeal.

This isolation from critical infrastructure brought on by a powerful hurricane grants visibility into the worst-case scenario. A major flaw in the disaster recovery plan was discovered by the staff working within Memorial Medical Hospital during the event, resulting in inflated consequences. The flaw was a lack of communication avenues to request assistance. The staff had to mitigate this disaster with no exterior aid, thus requiring difficult life decisions to be made.[10]

[10] Contreras, C. (2022, August 12). The harrowing true story behind five days at Memorial. E! Online. https://www.eonline.com/news/1341588/the-harrowing-true-story-behind-five-days-at-memorial

The Value of Partnerships

As previously stated, the interconnectedness of critical infrastructure runs so deep that all subsectors of critical infrastructure are usually referred to as one singular entity. As the implication suggests, CI is considered one multi-faceted entity and must be treated as such when discussing risk strategies. Therefore, security incidents in one subsector of critical infrastructure affect the larger entity as a whole. Despite the cascading consequences of incidents in CI, information sharing is somewhat siloed in individual sectors. This hinders the ability to complete information sharing for critical infrastructure. A problem that partnerships can solve.

Public-Private Partnerships are partnerships between private and public sectors defined as voluntary agreements between the public and private sectors enhance the coordination of remediation and restoration efforts exhibited by critical-infrastructure-owning entities in times of crisis[11]. Sector coordinating councils (SCCs) provide an opportunity for both private and public sector members to participate in security-related think tanks through working groups, advocate for policy at the federal level, and create crowdsourced best practices to evolve security risk management for the sector at large. Partnerships such as SCCs and the NCI allow critical infrastructure owners to participate in collaborative initiatives that can expedite remediation efforts. Such initiatives are prevalent in both crisis-prone areas such as Florida and collaborative economies such as the EU[12], but they can also be used as a mobilization tool in times of crisis. An example of a Public-Private Partnership in action was during the cleanup effort of Superstorm Sandy, where the private sector helped expedite the reconstruction of America's infrastructure[13].

Partnerships are not limited to agreements between public and private sector entities. Some partnerships are made between private sector entities in times of crisis for the betterment of the public. One example of such a partnership would be the transfer of patients from overcrowded small hospitals in northern California to Stanford Medical during the COVID-19 pandemic to ensure most patients received care. This action saved many lives and proved the value of partnerships in times of crisis[14].

Those who seek to do critical infrastructure harm prey on the lack of redundancy present in both the architecture and alerting mechanisms of private sector entities in the critical infrastructure space. Terrorist, radical, and underground guidebooks relaying methods of attacking infrastructure most often emphasize the confusion and turmoil following an attack. Such pieces of literature include The Anarchist's Cookbook and modern-day accelerationist publications such as The Hard Reset, which push radicalized individuals towards violence against the very infrastructure that props up the society they live in. An example of this is the 30-page manual within The Hard Reset that details how to destroy utility and communications infrastructure without getting caught[15]. The document recommends actions based on a perceived likely outcome of inflated confusion caused by non-redundancy.

An example of this would be tampering with a distribution transformer in a remote area of power-line coverage to cause a major outage followed by a lengthy effort to identify the faulty transformer. The massive outage and subsequent hunt for the damaged transformer being caused by damage to a publicly accessible pressure point is a recurring theme that drives recommendations on how best to attack critical infrastructure in extremist literature. A cross-sector analysis of The Hard Reset was published in July 2022 (available here for Health-ISAC members), the result of collaborative work by several ISACs and ISAOs and is useful to understand the ideas circulating in extremist communities that have aligned themselves against critical infrastructure.

[11] Public-Private partnerships. (n.d.). FDOT. https://www.fdot.gov/comptroller/pfo/p3.shtm

[12] ECI Directive. (n.d.). ENISA. https://www.enisa.europa.eu/topics/risk-management/current-risk/laws-regulation/national-security/eci-directive

[13] Rebuilding with Public-Private partnerships | RealClearPolicy. (2017, September 20). https://www.realclearpolicy.com/articles/2017/09/20/rebuilding_with_public-private_partnerships.html

[14] Stanford Medicine accepts hundreds of patient transfers to relieve regional hospitals during pandemic. (2021, January 14). News Center. https://www.med.stanford.edu/news/all-news/2021/01/stanford-medicine-aids-regional-hospitals-through-patient-transfers.html

[15] FLASH ALERT: HIGH RISK OF VIOLENCE WITH THE PUBLICATION OF "THE HARD RESET: a TERRORGRAM PUBLICATION. (2022, December 11). CTG. https://www.counterterrorismgroup.com/post/flash-alert-high-risk-of-violence-with-the-publication-of-the-hard-reset-a-terrorgram-publication

Conclusion

The interconnectedness of society has become so significant that it cannot be ignored. Now, if one large business or service provider gets hit with an incident, it is highly likely that the effects will ripple outwards, affecting adjacent businesses in the same and different industries[16]. This phenomenon is even more pronounced in critical infrastructure security due to the interdependence amongst the critical infrastructure sectors. Therefore, companies in both the public and private sectors should not rely on individualized security and information siloing as long-term solutions because this concept has been made obsolete by modern interconnectedness. A more collaborative approach is required to navigate the current risk landscape. Conducting organizational risk exercises and running through mock security incidents will help understand how information sharing organizations integrate into larger risk mitigation strategies. Collaborative partnerships and information sharing organizations with members in other critical infrastructure organizations are available should organizations choose. Participation in such organizations will likely increase long-term business resilience.

Whether the consequences impact an organization directly or indirectly through latent interdependence, cascading impacts from incidents in critical infrastructure are inevitable; therefore, it is imperative that the community comes together to defend it — because critical infrastructure security affects us all.

Further Reading

Coordinated Healthcare Incident Response Plan — A preparedness and response template created by the Health Sector Coordinating Council (HSCC) for disruptive cyber incidents involving health systems, hospitals, and clinics. Provides guidance for maintaining clinical and business operations as the effects of a cyber-attack threaten not only revenue but patient safety.

Health Industry Cybersecurity Practices 2023 — The HICP 2023 is an update to the 2019 HICP publication developed jointly by the HSCC and HHS. It provides executives, health care practitioners, providers, and health delivery organizations, such as hospitals, with best practices for managing cyber threats to safeguard patient safety.

Feedback and suggestions on this document are encouraged and welcome.

Please e-mail contact@H-ISAC.org

[16] Amadiegwu, A., Kihiu, M., & Simon, M. (2020). Mobilizing the Private Sector for Peace and Reconciliation. The Graduate Institute of Geneva